We claim:

1. A method for providing session protection for user privacy over a network, by means including at least a client and a remote server, wherein a user, using a client application, may submit a request through said client for a specified action to be performed in response to said request by said remote server, said user-submitted request comprising identity information that identifies the user making the request, and action information that specifies the action requested from said remote server by said user, and wherein said communications are provided in a secure and anonymous manner in that said action information is submitted to said remote server without revealing said identity information to said remote server, and in that only said client, and not any facility through which said action information or any response thereto passes in the course of being submitted to or received from said remote server, possesses both said identity information and said action information, said system comprising (in addition to said client and remote server):
   (a) separating, within said client application, said identity information and said action information from the user's information request, encrypting said identity information and said action information, and sending said identity information and said action information as so encrypted to an identity server;
   (b) decrypting, within said first intermediate server, said encrypted identity information but not said encrypted action information, and transmitting said encrypted action information to a second intermediate server;
   (c) decrypting, within said second intermediate server, said action information, transmitting said decrypted action information to said remote server, receiving the remote server's response, encrypting said remote server response, and transmitting said encrypted remote server response to said first intermediate server;
   (d) receiving, within said first intermediate server said encrypted remote server response from said second intermediate server, associating said encrypted remote server response with said identity information and sending said encrypted remote server response to said application; and
   (e) decrypting, within said client application, said remote server response and forwarding said decrypted remote server response to said client for presentation to said user.

2. A method for providing private storage of data within a network, to a user operating a computer connected to said network, said computer having a client application resident therein, there being available to said user on said network a server to provide storage services, said method for providing private storage comprising:
(a) generating within said client application a first encryption key and a first decryption key;
(b) encrypting said data within said client using said first encryption key;
(c) generating a data object identifier within said client application;
(d) creating a data object that contains said data object identifier and said encrypted data;
(e) sending said data object to said server;
(f) storing said data object in a database under the control of said server, using said data object identifier as a locator;
(g) writing said data object identifier to a user object within said client application;
(h) writing said first decryption key to said user object;
(i) generating within said client application a user object encryption key based on information private to said user and reproducible in future sessions by said user, in a manner such that said private information cannot practicably be derived from said user object encryption key;
(j) encrypting said user object with said user object encryption key;
(k) generating within said client application a user object identifier based on information private to said user and reproducible in future sessions by said user, in a manner such that said private information cannot practicably be derived from said user object identifier;
(l) associating said user object identifier with said user object;
(m) sending said user object and user object identifier to said server; and
(n) storing said user object in said database, using said user object identifier as a locator.

3. A method for private retrieval over a network of data that has been stored in accordance with the method of claim 2, to the user that stored said data, said user operating a computer connected to said network, said computer having a client application resident therein, there being available to said user on said network a server to provide storage services, said method for providing private retrieval of said data comprising:

(a) generating within said client application user object identifier in accordance with the same method and based on the same information that was used to generate the user identifier by which said data had previously been stored in accordance with claim 2;
(b) sending said user object identifier and a request for a user object to said server;
(c) if said user object identifier matches a user object identifier previously stored by said server, sending the requested user object to said client application, said requested user object comprising a data object decryption key and a data object identifier and being encrypted with a user object encryption key;
(d) generating within said client application a user object decryption key in accordance with the same method and based on the same information that was used to generate the user object encryption key in accordance with claim 2;
(e) decrypting said user object using said user object decryption key;
(f) selecting from said decrypted user object the data object identifier corresponding to the encrypted data desired to be retrieved;
(g) sending said data object identifier and a request for said encrypted data to said server;
(h) within said server, retrieving said encrypted data from a database under the control of said server, using said data object identifier as a locator;
(i) sending said encrypted data to said client application;
(j) reading said data object decryption key from said decrypted user object;
(k) decrypting said encrypted data with said data object decryption key; and
(l) making said decrypted data available to said user.

4. A method for providing private storage of data within a network, to a storing user operating a computer connected to said network, wherein access to said data is granted by said user to an accessing user, said computer having a client application resident therein, there being available to said storing user on said network a server to provide storage services, said method for providing private storage with access to said accessing user comprising:
(a) said storing user identifying the data to be stored and said accessing user, who is to have access thereto;

(b) generating within said client application a first encryption key and a first decryption key;
(c) encrypting said data within said client using said first encryption key;
(d) generating a data object identifier within said client application;
(d) generating a challenge public-private key pair for said data;
(e) reading with said client application an identifier for said accessing user;
(f) generating a coded user identifier from said user identifier in a manner such that said user identifier cannot practicably be deduced from said coded user identifier;
(g) sending said coded user identifier to said server together with a request for the accessing user's message queue public key;
(h) said server identifying the message queue public key associated with said coded user identifier and returning said message queue public key to said client application;
(i) creating a message object comprising said data object identifier, said first decryption key, and said private challenge key;
(j) encrypting said message object with said message queue public key;
(k) sending said encrypted message object to the message queue on said server associated with said coded user identifier;
(l) creating a data object comprising said data object identifier, said encrypted data, and said public challenge key;
(m)sending said data object to said server;
(n) said server storing said encrypted data in a database under the control of said server, using said data object identifier as a locator and maintaining an association with said public challenge key.

5. A method for private retrieval over a network of data that has been stored in accordance with the method of claim 4, to an accessing user granted access to said data in accordance with the method of claim 4, said accessing user operating a computer connected to said network, said computer having a client application resident therein, there being available to said accessing user on said network a server to provide storage services, said method for providing private retrieval of said data by said accessing user comprising:
(a) accessing user providing authentication token to client application;
(b) generating within said client application a user object identifier based on said authentication token in the same manner previously used to

generate the user object identifier associated with said accessing user on said server;

(c) sending said user object identifier and a request for a user object to said server;

(d) if said user object identifier matches a user object identifier previously stored by said second server, sending the requested user object to said client application, said requested user object comprising a reference to said accessing user's message queue on said server and a message queue decryption key;

(e) requesting said message queue from said server;

(f) said server retrieving said message queue from a database under control of said server, and returning said message queue to said client application, said message queue comprising a message object previously inserted in said message queue in accordance with claim 4;

(g) reading said message queue decryption key from said user object;

(h) decrypting said message object from said message queue with said message queue decryption key;

(i) reading said message object and obtaining therefrom the data object identifier for encrypted data that had been stored under control of said server in accordance with claim 4;

(j) generating a challenge request and forwarding said challenge request and said data object identifier to said server;

(k) said server encrypting said challenge with the public challenge key that was associated with said data object identifier in accordance with claim 4, and returning said encrypted challenge to said client application;

(l) reading said private challenge key from said message object;

(m) decrypting said encrypted challenge using said private challenge decryption key;

(n) returning said unencrypted challenge together with said data object identifier to said server;

(o) said server matching said challenge received with said challenge sent, and retrieving a data element associated with said data object identifier;

(p) sending said data element to said client application;

(q) reading said first decryption key from said message object; and

(r) decrypting encrypted data associated with said data element.

6. The method of claim 5, wherein said data element comprises the encrypted data stored in accordance with claim 4.;

7. The method of claim 5, wherein said encrypted data element comprises a handle conferring temporary approval to access one or more objects, whereby the encrypted data stored in accordance with claim 4 may be separately accessed in increments and decrypted.

8. The method of storage and retrieval and access control in accordance with claim 4 and claim 5, wherein the entity identified in said claims as the accessing user is a group of users defined in said second intermediate server, said group having a message queue and a challenge key, and wherein the users who were members of said group had in their user objects maintained within said second intermediate server a reference to said group and the group's challenge key, so as to enable said user to access any data for which access has been authorized to said group.

9. The method of any of claims 2, 3, 4, 5, 6, 7 or 8, wherein data transfer to and from said server is conducted in accordance with secure socket layer protocols.

10. The method of any of claims 2, 3, 4, 5, 6, 7 or 8, wherein said server is a second intermediate server in a system comprising first and second intermediate servers adapted to perform the method of claim 1, and wherein data transfer to and from said second intermediate server is conducted through a first intermediate server in accordance with the method of claim 1.

11. The method of claim 1 or claim 10 wherein said identity server and said action server are implemented as processes or threads which may execute on the same or different computers.

12. The method of claim 10 carried out in a distributed operating environment in which there are a plurality of users, a plurality of first intermediate servers and a plurality of second intermediate servers, all communicating in accordance with the method of claim 1.